

## REMARKS

Claims 1-8 and 14-17 were pending prior to entering this amendment. Claims 1-8 and 14-17 stand rejected. The specification is objected to.

Because the cited prior art fails to teach elements of the claims, no amendments to the claims are deemed necessary and none made except for a clarification amendment to claim 3. At least in light of the above amendments and the foregoing remarks, issuance of the allowed claims is respectfully requested.

### Summary

The newly cited Wagner reference is distinguished from the claims on the following grounds:

- As an anti-eavesdropping measure, Wagner teaches away from operating cookie processing script on the visitor computer
- Because Wagner is anti-cookie, it would not be obvious to combine Wagner with other prior art that DO use cookies.
- Wagner's discussion of cookies in its Background section involve sending cookie data, set in advance, from the cookie server to the visitor computer; cookies are thus not set at the visitor computer in view of browsing data—that is, the cookie processing script is not operated on the web browsing data.

The Bharat reference fails to teach all elements of independent claim 14, namely:

- The Examiner has admitted in a past response that the Bharat reference fails to teach the method of embedding data mining script within a web page and operating the data mining script on the client node.

The Pogue reference fails to teach additional elements of claim 16, namely:

- Pogue only transmits a new cookie from the tracker 310 to the browser 302, thereby replacing the cookie on the visitor computer rather than attaching the cookie values to an image request associated with a designated source.

*A. The specification provides adequate support for the claim limitation, “operating the data mining code on the visitor computer to obtain web browsing data.”*

All pending claims have been rejected under 35 U.S.C. §112, first paragraph, on the grounds that the claims contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Applicants traverse this rejection on the grounds that the application includes JavaScript code in an Appendix that successfully operates to implement the functions recited in the claims.

This is not simply a matter of saying ‘what’ you want to do without providing the ‘how’—instead, the specification includes real code that operates in the fashion stated. One knowledgeable in the art would thus have a working example of code that is capable of “operating on the visitor computer to obtain web browsing data.” The code included in Appendix A sets variables according to data collected by operation of the code, including the following:

Examples of web browsing data obtained  
by data mining code of Appendix A

- |                |                    |                    |
|----------------|--------------------|--------------------|
| • referrer     | • screenResolution | • LastOrderRef     |
| • userLanguage | • VisitDate        | • NewVisitInterval |
| • platform     | • PageDepth        | • PageLoadTime     |

The language “...to obtain web browsing data was original claim language in the patent application and thus part of the specification as filed.” Furthermore, one knowledgeable in the art would recognize that the data variables gathered such as those named above correspond to “web browsing data.” This data is also referred to as “new events” in the specification (page 11, line 44), e.g. new browsing data that occurred since the cookie was last set, and to the JavaScript code described at several other places within the specification, e.g. page 1, lines 25-30. A subroutine then writes a new cookie value in view of the old cookie and the new events.

The Examiner has chosen to treat the “operating the data mining code” and “operating the cookie processing script” as the same limitation. While the code listed in the Appendix combines these two features, it would be both a technical and legal error to consider both functions to be the same as such can be enabled by entirely separate subroutines without departing from the spirit of the invention.

*B. The teachings of the newly cited Wagner reference seek to prevent operation of cookies, not implement them as in the present invention*

---

Responsive to arguments made in a recent Pre-Appeal Brief, the Examiner has now withdrawn rejections to the claims made in view of the Ludewig reference. The Examiner now cites to a new reference, U.S. Patent No. 6,085,224 (Wagner). Claim 1 has been rejected under 35 U.S.C. §102(e) as being anticipated by the Wagner reference. Claims 2-8 have been rejected under §103(a) under Wagner in view of other references as follows:

- Claims 2 and 5-8 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Wagner as applied to claim 1 above, and further in view of U.S. Patent No. 6,112,240 (Pogue, et al.).
- Claim 3 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Wagner and Pogue as applied to claims 1 and 2 above, and further in view of U.S. Patent Application Publication No. 2002/0040395 (Davis, et al.).
- Claims 4 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Wagner, Pogue and Davis as applied to claims 1-3 above, and further in view of U.S. Patent No. 6,374,359 (Shrader, et al.).
- Claim 5 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Wagner, Pogue and Davis.

The claims are being rejected strictly on the disclosure contained in the Wagner reference's Background section rather than in its improvement over the prior art.

Whereas the present invention is directed to tracking user browsing behavior, the Wagner reference seems dedicated to preventing such tracking. In its Background Section, Wagner references the potential harm caused by cookies:

While the storage of a cookie file may appear harmless, it is nevertheless the unauthorized storage of data on another's computer and the file may be used for tracking the user and his or her requests for information from the server site without the user's knowledge or permission. [Wagner, col. 2, lines 49-53]

Wagner then notes that prior art programs have been developed that monitor the HTTP headers and delete cookie data from these headers. These prior art programs, however, are incapable of deleting either inbound or outbound cookie data when sent via interpretive languages such as Javascript:

While these previously known programs may be used to selectively notify a user of the presence of cookie data from an HTTP header, these programs do not detect other hidden data which a user may want to know is being passed to the user's browser or want to delete from an HTML file or request. [Wagner, col. 3, lines 8-14]

While applets have a number of beneficial purposes, they may also cause problems. For example, a JAVA applet may be imbedded in an HTML file, sent to a user's computer and executed by an interpreter in the browser without the user's knowledge...Additionally, these interpretive language programs may include cookie commands that identify tracking data as discussed above. [Wagner, col. 3, lines 34-41]

The end result is that since the cookie commands are not part of the HTTP header, then prior art programs that would ordinarily be used to detect and delete cookie data are incapable of detecting cookie commands. Wagner then mentions that browsers have been rewritten to include

a feature that disable the execution of interpretive programs and cookie commands, similar to that described in Applicant's Background section on page 3 of the patent application. Whereas the present invention seeks a workaround to this type of modified browser function, the Wagner reference seeks to enhance the exclusion of cookie commands by adding a user notification step:

What is needed is a program which notifies the user of detected interpretive programs and cookie commands without modifying the browser program. What is needed is a way to restrict access to resources or data on a computer when the computer is in communication with another computer. [Wagner, col. 4, lines 4-9]

The present invention and Wagner thus appear to be on different sides with respect to the issue of cookies. Whereas the present invention seeks to store a cookie on a web site visitor's computer, the Wagner reference seeks to prevent that from happening.

*C. Wagner does not teach including data mining code and cookie processing script within a web page per claim 1*

---

Claim 1 includes the step of storing a web page on a server where the web page includes data mining code and cookie processing script. Despite the additional overhead of adding script to a web page and thus increasing download times, including the script gives the web site owner an advantage of gleaning web site traffic information from the visitor. Such information would assist the web site owner in tailoring their web site to reach and appeal to the broadest range of customers.

In contrast to the present invention, Wagner discloses a program that is used to delete cookies and/or prevent them from operating. Accordingly, the web site owner would gain no additional knowledge from the web site visitor by embedding the Wagner program into their web pages. There would then be no motivation for including a cookie disabling and notification program such as described in Wagner within a web page as this works counter the web site owner's desire to obtain information from the visitor, whether voluntarily or automatically. It is thus factual error to ascribe the teaching of embedding data mining code and cookie processing script into the web page itself.

Although the Wagner invention itself does not teach including additional script within a web page, prior art methods noted in the Wagner Background section do. The Examiner cites to col. 3, lines 15-41 of the Wagner Background section in which a JAVA applet within an HTML file is executed by the browser to include a cookie command. There is no reason to believe,

however, that these cookie commands are nothing more than standard cookie storing commands. The operation of such standard cookies is described in applicant's patent application, particularly on page 5. In such standard cookies commands, name-value pairs (e.g. UserID and a long hexadecimal number) are generated according to an algorithm programmed in the cookie server associated with the domain web site. This unique name-value pair is then stored in a cookie file at the visitor computer and sent back to the domain that set the cookie upon each request for information, like an ID badge at a conference. The domain then knows who is requesting the information and can track a visitor's behavior at the web server across several visits. All traffic tracking information is conducted at the web server. There is no mechanism within Wagner for allowing a third party to track the information (e.g. claim 2).

Standard cookies and cookie-setting processes do not operate cookie processing script on the web browsing data to obtain new cookie values (e.g. claim 1). Instead, cookie values are set in advance by a cookie server. Such values are not determined at the visitor computer, and such values are not set in consideration of the web browsing data obtained at the visitor computer via the data mining code. Features of the claim are thus missing from Wagner and thus the prior art of record. Reconsideration and removal of the rejection is respectfully requested.

*D. Bharat still fails to teach elements of claim 14 on its own*

Whereas claims 14-15 had previously been rejected under 35 U.S.C. §103(a) in view of U.S. Patent No. 6,810,395 (Bharat) and another reference (l'Etraz), these claims are now rejected under 102(e) solely in view of Bharat. Claims 16 and 17 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Bharat as applied to claim 14 above, and further in view of Pogue.

The Examiner had previously held, in an Office Action dated May 18, 2007, that Bharat fails to teach the method of embedding data mining script within a web page and operating the data mining script on the client node. Bharat still fails this test, making rejection of the claims under §102(e) inappropriate. There is no basis for treating

Claim 14 has been amended in a previous action to cite that the cookie processing script is associated with a different domain than the web page—that is, where the web page provider and the (web tracking) service provider are different entities. Neither Bharat (or the old-cited l'Etraz) contemplate this feature.

*E. Pogue does not attach the new cookie values to an image request associated with a designated URL source (Claim 16)*

---


Claim 16 includes the steps of “attaching the new cookie values to an image request” associated with a designated URL source, and “sending the image request to the URL source.” An example of this action would be to send the newly provided cookie values from the visitor computer to a tracking computer.

Pogue does not describe this feature. Citing to the portion identified by the Examiner (Pogue, Col. 7, lines 11-22), Pogue instead only transmits a new cookie from the tracker 310 to the browser 302 thereby replacing the cookie on the visitor computer. Pogue does not teach that the cookie is then attached to an image request associated with a designated source. Reconsideration and allowance of the claims is thus respectfully requested.

For the foregoing reasons, reconsideration and allowance of claims 1-8 and 14-17 of the application as amended is requested. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

  
\_\_\_\_\_  
Scott A. Schaffer  
Reg. No. 38,610

MARGER JOHNSON & McCOLLOM, P.C.  
210 SW Morrison Street, Suite 400  
Portland, OR 97204  
503-222-3613  
**Customer No. 20575**